

# Strengthening Your Compliance Program Through Effective Annual Compliance Reviews Under Rule 206(4)-7



Jin Lien

September 16, 2025

The Investment Advisers Act of 1940 was created to put investors first, ensuring that Registered Investment Advisers (RIAs) act with integrity and in their clients' best interests.

One of its cornerstone rules, Rule 206(4)-7, requires RIAs to adopt written compliance policies and procedures, appoint a Chief Compliance Officer (CCO), and review the effectiveness of their compliance program at least annually.

Too often, firms approach the annual review as a routine exercise, a formality to “check the box”, but regulators expect more. A meaningful review should be tailored to the firm's risk profile and informed by insights gathered across the business, including input from senior leadership and staff.

The annual review should be viewed as a critical opportunity to strengthen the compliance program and demonstrate regulatory readiness. A well-structured approach includes the following steps:

## Step 1: Start With a Risk Assessment

A meaningful annual review begins with a clear understanding of the firm's risk profile. Conducting a structured risk assessment, supported by input from key business personnel, helps identify the compliance areas most vulnerable to regulatory scrutiny, operational weaknesses, or control gaps.

Key factors that commonly influence a firm's risk profile include:

- Investment strategies and fund structures
- Types of clients and investors
- Relationships with third parties (administrators, placement agents, service providers)
- Fee arrangements and potential conflicts of interest
- Employee turnover and training practices
- Marketing activities and use of digital channels
- Adoption of emerging technologies (e.g., AI tools, digital communications)

Revisiting and updating the risk assessment each year ensures that the compliance roadmap remains aligned with both regulatory expectations and the realities of an evolving market environment.

## Step 2: Implement Risk-Based Testing

Once risk areas have been identified, the next step is to design a targeted testing program. The goal is not to test every policy in the manual, but to focus resources on the areas that matter most:

- High-risk areas (such as custody, marketing, and personal trading) should be reviewed annually
- Lower-risk areas can be incorporated on a rotating, multi-year cycle
- Testing should be sample-based, with sample sizes tied to how often the control operates (daily, monthly, quarterly, etc.).

For private fund managers, regulators often focus on specific areas where conflicts of interest and disclosure issues are most likely to arise. Incorporating testing around these topics helps ensure controls are functioning effectively and demonstrates that the compliance program is aligned with SEC expectations.

Examples of risk-based testing areas include:

Area	What to Test
Expense Allocations	Review expenses to confirm proper expense allocation between the fund and management company, and consistency with disclosures in fund governing documents
Valuation Controls	Examine selected valuations to ensure methodologies are applied consistently and in accordance with written policy
Side Letter Compliance	Verify that preferential terms granted to certain investors (e.g., fee breaks, reporting rights) are tracked and honored
Cross-Trades / Principal Transactions	Confirm that transactions received required approvals, were documented and disclosed properly, and complied with fiduciary obligations
MNPI / Insider Trading Controls	Test handling of material non-public information (MNPI), including usage of expert networks, restricted lists, and employee trading activity

This structured, risk-based approach allows firms to allocate compliance resources effectively and provides regulators with clear evidence that controls are being tested in the areas of greatest importance.

## Step 3: Document, Remediate, and Evolve

The value of an annual review lies not just in testing but in how the results are used. Regulators expect firms to move beyond confirming that policies exist; they want evidence that compliance programs are actively improving.

An effective process should include:

- Clear documentation of testing results
- Identification of issues, with remediation steps assigned to responsible owners
- Adjustments to policies, controls, or oversight based on findings
- Integration of findings into the following year's risk assessment.

By treating the review as an ongoing cycle of assessment, testing, remediation, and refinement, firms demonstrate a mature compliance culture that adapts to regulatory expectations and strengthens operational resilience.

## Why This Matters

A robust annual review goes beyond checking a regulatory box to help:

- Protect investors and safeguards firm reputation
- Demonstrate to regulators that your compliance program is effective and evolving
- Provide clients and investors with greater confidence in the firm's oversight
- Reinforce a culture of accountability and compliance within the organization

## Enhancing Compliance Through Ongoing Review

Annual reviews are not simply about satisfying a regulatory requirement. They provide an opportunity to evaluate the effectiveness of the compliance program, highlight areas for enhancement, and demonstrate to regulators and investors that fiduciary obligations are taken seriously.

When approached as an ongoing cycle of risk assessment, targeted testing, documentation, and remediation, the review becomes a tool for continuous improvement. A well-structured process helps firms adapt to regulatory change, strengthens operational resilience, and instills confidence that the compliance program can withstand regulatory inquiries and examinations.

## How Waystone Can Help

Waystone delivers tailored comprehensive annual compliance reviews designed to help firms stay ahead of evolving SEC regulatory requirements. Supported by a dedicated team of compliance specialists with deep industry knowledge, we work closely with firms to assess their risk profiles, evaluate the effectiveness of compliance programs, and ensure ongoing adherence to SEC obligations.

If you have any questions about any of the themes raised in this article or to learn more about how Waystone can help you meet SEC expectations, please contact your usual Waystone representative or reach out to our [US Compliance Solutions](#) team below.

[Contact Us](#) →